



Attorney Docket No.: 06944.0037
Customer No.: 22,852
Serial No.: 09/885,959
Filed: June 22, 2001

- 19 -

ABSTRACT OF THE DISCLOSURE

This invention provides a method for accelerating multiplication of an elliptic curve point $Q(x,y)$ by a scalar k , the method comprising the steps of selecting an elliptic curve over a finite field F_q where q is a prime power such that there exists an endomorphism Ψ , where $\Psi(Q)=\lambda.Q$ for all points $Q(x,y)$ on the elliptic curve: and using smaller representations k_i of the scalar k in combination with the mapping Ψ to compute the scalar multiple of the elliptic curve point Q .

09885959-101501

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

215718-1